PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-212730
(43)Date of publication of application : 06.08.1999

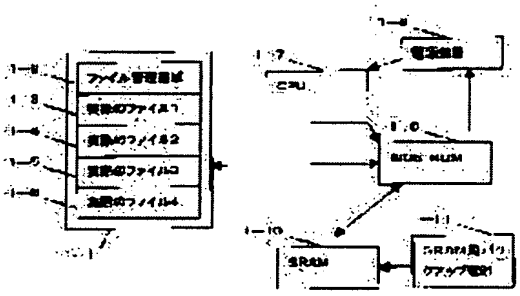
(51)Int.Cl. G06F 3/06

(21)Application number : 10-009376
(22)Date of filing : 21.01.1998

(71)Applicant : MATSUSHITA ELECTRIC IND CO LTD
(72)Inventor : KOBAYASHI TAKASHI

(54) METHOD AND DEVICE FOR PREVENTING INFORMATION LEAK OF SECONDARY STORAGE DEVICE

(57)Abstract:
PROBLEM TO BE SOLVED: To prevent information leak when a secondary storage device is stolen, etc., by copying a part of contents of the secondary storage device to nonvolatile memory when power source is off and writing invalid data to a part of the contents of the secondary storage device.
SOLUTION: In a leading area 1-2 of a hard disk drive 1-1 file management information is stored. When the power source is off, interruption of power source off from a power supply device 1-9 occurs and it is notified to a CPU 1-7. The interruption makes the software of a BIOSROM 1-8 operate and copies data in an area 1-2 to an SRAM 1-10. Next, the software of the BIOSRAM 1-8 writes invalid data in the area 1-2 and makes the device 1-9 execute an actual power source off operation after it is finished. When the drive 1-1 is stolen and is connected to another personal computer, it is actually impossible to start an OS and to read file contents because management information 1-2 is destroyed.



LEGAL STATUS

[Date of request for examination] 17.06.1998
[Date of sending the examiner's decision of rejection] 17.08.1999
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's

decision of rejection]
[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号

特開平11－212730

(43)公開日　平成11年(1999)８月６日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｇ０６Ｆ　3/06	３０４	Ｇ０６Ｆ　3/06	３０４Ｈ

審査請求　有　　請求項の数６　ＯＬ　（全６頁）

(21)出願番号　特願平10－9376

(22)出願日　平成10年(1998)１月21日

(71)出願人　000005821
松下電器産業株式会社
大阪府門真市大字門真1006番地

(72)発明者　小林　敬
大阪府門真市大字門真1006番地　松下電器産業株式会社内

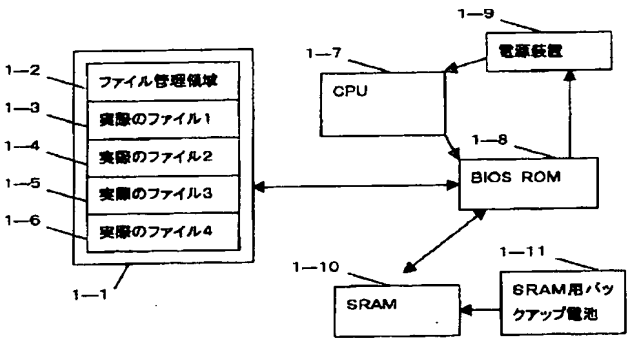
(74)代理人　弁理士　岩橋　文雄　（外２名）

(54)【発明の名称】　二次記憶装置の情報漏洩防止方法および装置

(57)【要約】

【課題】　情報処理機器または二次記憶装置が盗難された場合に、二次記憶装置の内容にアクセスできないようにすることを目的とする。

【解決手段】　電源オフ時に二次記憶装置中のファイル管理領域をＳＲＡＭに待避し、ファイル管理領域の内容を破壊してから実際に電源をオフする。電源オン時にファイル管理領域を復旧する。二次記憶装置が電源オフ中に盗難されても、ファイル管理領域が無効になるため内容にアクセスできない。また、パスワード保護を併用しパスワードを同じＳＲＡＭに保存しておくことで、情報処理機器が盗難されても二次記憶装置の内容にアクセスさせないようにできる。



【特許請求の範囲】
【請求項１】電源オフ時に二次記憶装置のデータ退避対象領域のデータを退避データとして不揮発性メモリーに退避するデータ退避手順と、前記データ退避手順によるデータ退避後に前記退避データと異なるデータを前記データ退避対象領域に書き込むデータ書き換え手段と、電源オン時に前記退避データを前記データ退避対象領域に書き込むデータ復帰手順を有する二次記憶装置の情報漏洩防止方法。
【請求項２】データ退避対象領域が二次記憶装置の先頭領域である請求項１記載の二次記憶装置の情報漏洩防止方法。
【請求項３】データ退避対象領域が、一つ又は複数の区画に分割された二次記憶装置の区画の先頭領域である請求項１記載の二次記憶装置の情報漏洩防止方法。
【請求項４】電源オフ時に二次記憶装置のデータ退避対象領域のデータを退避データとして不揮発性メモリーに退避するデータ退避手段と、前記データ退避手段によるデータ退避後に前記退避データと異なるデータを前記データ退避対象領域に書き込むデータ書換手段と、電源オン時に前記退避データを前記データ退避対象領域に書き込むデータ復帰手段を有する二次記憶装置の情報漏洩防止装置。
【請求項５】データ退避対象領域が二次記憶装置の先頭領域である請求項４記載の二次記憶装置の情報漏洩防止装置。
【請求項６】データ退避対象領域が、一つ又は複数の区画に分割された二次記憶装置の区画の先頭領域である請求項４記載の二次記憶装置の情報漏洩防止装置。
【請求項７】電源オン時にユーザー認証のためにパスワード情報を使用するパスワード保護手順を有し、不揮発性メモリーに前記パスワード情報を保持する手順を有する請求項１記載の二次記憶装置の情報漏洩防止方法。
【請求項８】データ退避対象領域が二次記憶装置の先頭領域である請求項７記載の二次記憶装置の情報漏洩防止方法。
【請求項９】データ退避対象領域が、一つ又は複数の区画に分割された二次記憶装置の区画の先頭領域である請求項７記載の二次記憶装置の情報漏洩防止方法。
【請求項１０】電源オン時にユーザー認証のためにパスワード情報を使用するパスワード保護手段を有し、不揮発性メモリーに前記パスワード情報を保持する請求項４記載の二次記憶装置の情報漏洩防止装置。
【請求項１１】データ退避対象領域が二次記憶装置の先頭領域である請求項１０記載の二次記憶装置の情報漏洩防止装置。
【請求項１２】データ退避対象領域が、一つ又は複数の区画に分割された二次記憶装置の区画の先頭領域である請求項１０記載の二次記憶装置の情報漏洩防止装置。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は情報処理装置における情報漏洩防止に関するものである。
【０００２】
【従来の技術】従来、情報漏洩防止のためには、情報処理装置の電源オンにおけるパスワード保護が行われている。
【０００３】
【発明が解決しようとする課題】電源オンにおけるパスワード保護では、二次記憶装置を盗難された場合、情報の漏洩が発生する。また、パスワードを記憶している不揮発性メモリーの内容保持のための電池を抜く、あるいは物理的に破壊するなどしてそのデータを消滅させれば容易にパスワード保護を無効とできる。
【０００４】情報処理装置の二次記憶装置に機密性の高い情報を保存することが一般的になっているため、盗難時等でも情報の漏洩がないように防止する対策が要求されている。
【０００５】本発明は、二次記憶装置の盗難時等の情報漏洩防止を目的とする。
【０００６】
【課題を解決するための手段】この課題を解決するために本発明は、電源オフしたときに二次記憶装置の内容を無効にし、電源オン時に復帰させるように構成したものである。
【０００７】これにより、正常使用状態の使い勝手の低下をもたらさずに、盗難時の情報漏洩防止効果が得られる。
【０００８】本発明の請求項１に記載の発明は、二次記憶装置と、不揮発性メモリーとを有する情報処理装置で、電源オフのとき二次記憶装置の内容の一部を不揮発性メモリーにコピーし、二次記憶装置の内容の一部に無効なデータを書き込み、また電源オンのときに不揮発性メモリーにコピーしておいた情報を二次記憶装置に書き込むことで、電源オフの間に二次記憶装置が盗難されても内容が読めないという作用を有する。
【０００９】請求項２に記載の発明は、請求項１記載の二次記憶装置の内容の一部として二次記憶装置の先頭のデータを使用する情報漏洩防止方法であり、通常二次記憶装置の管理情報などの重要なデータが保存されている先頭データを無効にすることにより、電源オフの間に二次記憶装置が盗難された時にデータ保護をさらに確実にするという作用を有する。
【００１０】請求項３に記載の発明は、請求項１記載の二次記憶装置が１つ又は複数の区画に分割されて管理されているとき、二次記憶装置の内容の一部として各区画の先頭位置を使用する情報漏洩防止方法であり、通常区画の管理情報などの重要なデータが保存されている各区画の先頭データを無効にすることにより、電源オフの間に二次記憶装置が盗難された時にデータ保護をさらに確

実にするという作用を有する。

【００１１】請求項４ないし６に記載の発明は、請求項１ないし３に記載の手順を有する情報処理装置である。

【００１２】請求項７ないし９に記載の発明は、電源オン時にユーザー認証のためのパスワード保護手順を有した請求項４ないし６に記載の発明であり、パスワードと退避データを同じ不揮発性メモリーに書き込むことにより、パスワードを破壊するという不正な試みと同時に退避データを破壊し、情報漏洩を防止するという作用を有する。

【００１３】請求項１０ないし１２に記載の発明は、請求項７ないし９に記載の手順を有する情報処理装置である。

【００１４】

【発明の実施の形態】以下、本発明の実施の形態について、図１から図３を用いて説明する。

【００１５】（実施の形態１）図１はハードウェア構成を示す。

【００１６】図２は通常処理の流れを示し、図２において処理Ｓ２０５は、ハードディスク装置の内容の一部を不揮発性メモリーにコピーし、処理Ｓ２０６でハードディスク装置の内容の一部に無効なデータを書き込み、あわせて電源オフの前にハードディスク装置の内容の破壊と、復帰準備を行う。処理Ｓ２０９で電源オン時に、ハードディスク装置の内容を復帰させる。処理Ｓ２１０で、正常にＯＳを起動することができる。

【００１７】図３は電源オフ中にハードディスク装置が盗難された時の流れを示し、処理Ｓ３０５ないしＳ３０６を経ているため、盗難先での不正なアクセスによっても情報の漏洩がないという作用を持つ。

【００１８】なお、以上の説明では、二次記録装置をハードディスク装置で構成した例で説明したが、脱着可能な二次記録装置についても同様に実施可能である。

【００１９】次に、本発明の具体例を説明する。

【００２０】

【実施例】（実施例１）図１は請求項５に記載の情報漏洩防止装置のハードウェア構成を示す。ハードディスク装置１－１の先頭１－２には、ファイル管理情報が保存されている。電源オフ時に電源装置１－９から電源オフの割り込みが発生し、ＣＰＵ１－７に通知される。この割り込みによってＢＩＯＳＲＯＭ１－８のソフトウェアが動作し、１－２のデータをＳＲＡＭ１－１０にコピーする。次にＢＩＯＳＲＯＭ１－８のソフトウェアは、無効なデータを１－２に書き込み、その終了後電源装置１－９に実際の電源オフ動作を実行させる。

【００２１】この状態でハードディスク装置１－１が盗難され、別のパソコンに接続された場合、ハードディスク装置１－１のファイル内容はそのまま記録されているが、管理情報である１－２が破壊されているので、実際にはＯＳの起動やファイル内容の読み込みはできない。

【００２２】盗難がなく、次回通常通り電源オンすると、同様にＢＩＯＳＲＯＭ１－８のソフトウェアが動作し、ＳＲＡＭ１－１０にコピーしておいたデータを１－２に書き込んでからＯＳの起動を行うので、正常な動作となる。

【００２３】なお、この実施例では電源オフの期間、バックアップ電池１－１１によってＳＲＡＭ１－１０の内容を保持しているが、電池によるバックアップの不要なメモリー（フラッシュロムなど）、あるいは電池とメモリーが一体となった一体型メモリーでも同様の効果が得られる。

【００２４】（実施例２）実施例１と同様のハードウェア構成において、パスワード情報をＳＲＡＭ１－１０に保持しているとして、請求項８の情報漏洩防止装置の実施例である。ハードディスク装置１－１のみの盗難ではなく、パソコン全体が盗難された場合を説明する。

【００２５】盗難者はパスワードを知らないので、パスワードを無効にするためにバックアップ電池１－１１をＳＲＡＭ１－１０から切り離し、ＳＲＡＭ１－１０に保持されているパスワード情報を消去しようとする。これによって、パソコンの起動までは可能となる。

【００２６】ところが、パスワード情報の消去と同時にＳＲＡＭ１－１０に保持されていたファイル管理情報も消去されるので、ＢＩＯＳＲＯＭソフトは１－２のデータを復帰することができず、ＯＳの起動やファイル内容の読み込みはできない。

【００２７】

【発明の効果】以上のように本発明によれば、情報処理装置ないし情報記憶媒体が盗難に遭ってもその内容が不正アクセスされないという有利な効果が得られる。

【図面の簡単な説明】

【図１】本発明の実施例のハードウェア構成図

【図２】本発明の一実施の形態による正常処理のフローチャート

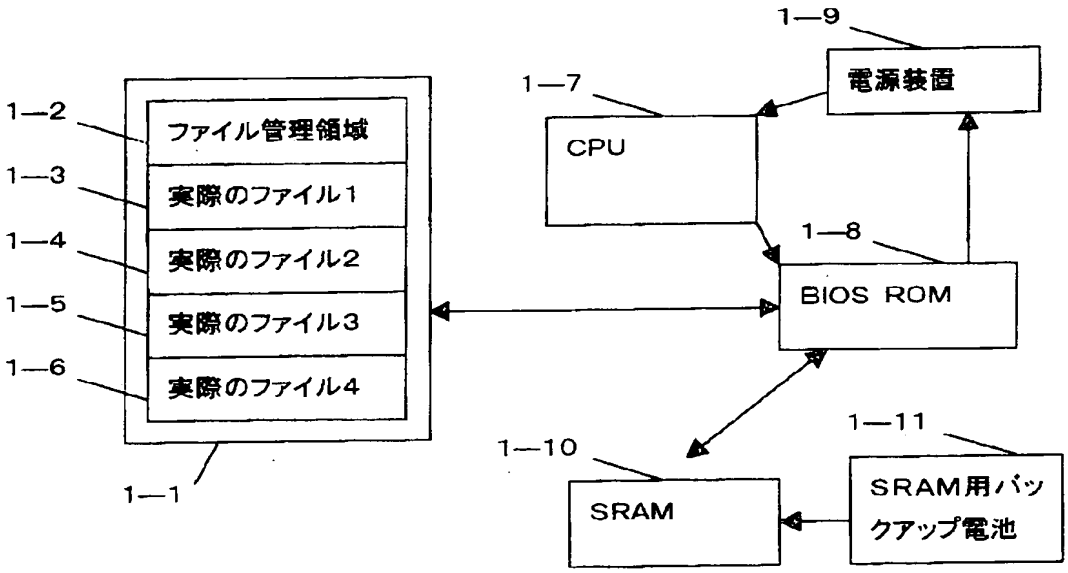
【図３】本発明の一実施の形態による盗難時処理のフローチャート

【符号の説明】

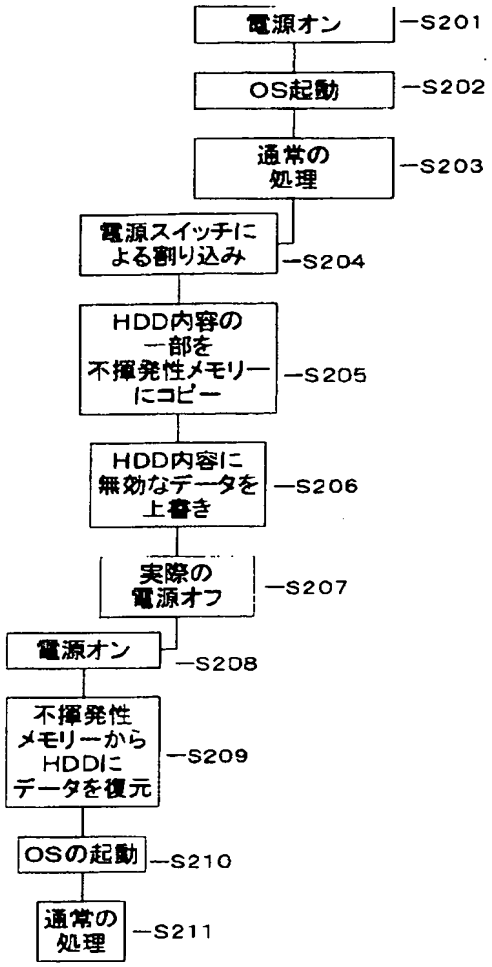
１－１　ハードディスク装置
１－２　ファイル管理情報データ
１－３～１－６　実際のファイル
１－７　ＣＰＵ
１－８　ＢＩＯＳＲＯＭ
１－９　電源装置
１－１０　ＳＲＡＭ
１－１１　ＳＲＡＭバックアップ用電池
Ｓ２０１　電源オン
Ｓ２０２　ＯＳ起動
Ｓ２０３　通常の処理
Ｓ２０４　電源スイッチによる割り込み
Ｓ２０５　ハードディスク装置のデータ待避対象領域の

不揮発性メモリーへのコピー
Ｓ２０６　ハードディスク装置のデータ待避対象領域への無効データの書き込み
Ｓ２０７　電源オフ
Ｓ２０８　電源オン
Ｓ２０９　不揮発性メモリーからデータ待避対象領域へのデータ復帰処理
Ｓ２１０　ＯＳの起動
Ｓ２１１　通常の処理
Ｓ３０１　電源オン
Ｓ３０２　ＯＳ起動
Ｓ３０３　通常の処理
Ｓ３０４　電源スイッチによる割り込み
Ｓ３０５　ハードディスク装置のデータ待避対象領域の不揮発性メモリーへのコピー
Ｓ３０６　ハードディスク装置のデータ待避対象領域への無効データの書き込み
Ｓ３０７　電源オフ
Ｓ３０８　ハードディスク装置の盗難
Ｓ３０９　盗難されたハードディスク装置の別パソコンでの起動
Ｓ３１０　ＯＳ非起動
Ｓ３１１　内容不読

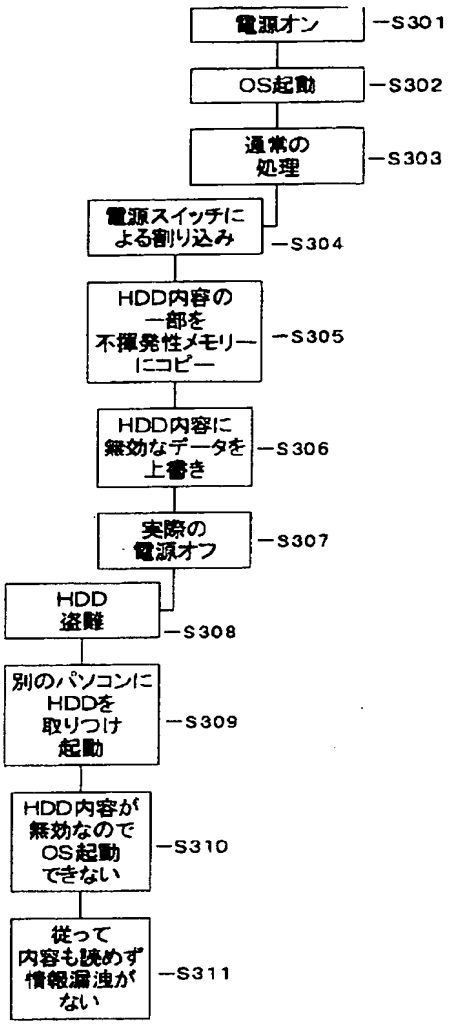
【図１】



【図２】



【図３】



【手続補正書】
【提出日】平成１０年１２月９日
【手続補正１】
【補正対象書類名】明細書
【補正対象項目名】特許請求の範囲
【補正方法】変更
【補正内容】
【特許請求の範囲】
【請求項１】　電源オフ時に二次記憶装置のデータ退避対象領域のデータを退避データとして不揮発性メモリーに退避するデータ退避手順と、前記データ退避手順によるデータ退避後に前記退避データと異なるデータを前記データ退避対象領域に書き込むデータ書き換え手順と、電源オン時に前記退避データを前記データ退避対象領域に書き込むデータ復帰手順と、電源オン時にユーザー認証のためにパスワード情報を使用するパスワード保護手順と、前記不揮発性メモリーに前記パスワード情報を保持するパスワード保持手順から成る二次記憶装置の情報漏洩防止方法。
【請求項２】　データ退避対象領域が二次記憶装置の先頭領域である請求項１記載の二次記憶装置の情報漏洩防止方法。
【請求項３】　データ退避対象領域が一つ又は複数の区画に分割された二次記憶装置の各区画の先頭領域である請求項１記載の二次記憶装置の情報漏洩防止方法。
【請求項４】　電源オフ時に二次記憶装置のデータ退避対象領域のデータを退避データとして不揮発性メモリーに退避するデータ退避手段と、前記データ退避手段によるデータ退避後に前記退避データと異なるデータを前記データ退避対象領域に書き込むデータ書き換え手段と、電源オン時に前記退避データを前記データ退避対象領域

に書き込むデータ復帰手段と、電源オン時にユーザー認証のためにパスワード情報を使用するパスワード保護手段と、前記不揮発性メモリーに前記パスワード情報を保持するパスワード保持手段を有する二次記憶装置の情報漏洩防止装置。

【請求項５】　データ退避対象領域が二次記憶装置の先頭領域である請求項４記載の二次記憶装置の情報漏洩防止装置。

【請求項６】　データ退避対象領域が一つ又は複数の区画に分割された二次記憶装置の各区画の先頭領域である請求項４記載の二次記憶装置の情報漏洩防止装置。